Putting things to work: social and policy challenges for the Internet of things

William H. Dutton

William H. Dutton is a Professor and based at Oxford Internet Institute, University of Oxford, Oxford, UK.

Abstract

Purpose – *This paper aims to provide a critical assessment of the Internet of things (IoT) and the social and policy issues raised by its development. While the Internet will continue to become ever more central to everyday life and work, there is a new but complementary vision for an IoT, which will connect billions of objects – "things" like sensors, monitors, and radio-frequency identification devices – to the Internet at a scale that far outstrips use of the Internet as we know it, and will have enormous social and economic implications.*

Design/methodology/approach – *It is based on a review of literature and emerging developments, including synthesis of a workshop and discussions within a special interest group on the IoT.*

Findings – *Nations can harvest the potential of this wave of innovation not only for manufacturing but also for everyday life and work and the development of new information and services that will change the way we do things in many walks of life. However, its success is not inevitable. Technical visions will not lead inexorably to successful public and private infrastructures that support the vitality of an IoT and the quality of everyday life and work. In fact, the IoT could undermine such core values as privacy, equality, trust and individual choice if not designed, implemented and governed in appropriate ways.*

Research limitations/implications – *There is a need for more multi-disciplinary research on the IoT.*

Practical implications – *Policymakers and opinion formers need to understand the IoT and its implications.*

Social implications – *If the right policies and business models are developed, the IoT will stimulate major social, economic and service innovations in the next years and decades.*

Originality/value – *This paper pulls together discussions and literature from a social science perspective, as one means to enable more multidisciplinary studies of emerging developments.*

Keywords *Open systems, Communication technologies, Surveillance, Internet of Things, Consumers, Social behaviour*

Paper type *Conceptual paper*

Received 20 September 2013
Revised 18 February 2014
Accepted 5 March 2014

The author wishes to thank a number of colleagues for their advice and recommendations of key reports and other publications, including John Varney, Susan Clark and all members of the Technology Strategy Board's Special Interest Group on the IoT. The author is particularly grateful to Miranda Mowbray, Rich Ling, Barbara Ball and several anonymous reviewers for their comments on an earlier draft.

Introduction

The Internet has become increasingly significant for social and economic development worldwide, and is likely to become ever more central to everyday life and work, in line with conceptions of digital economies. A new stage of its development could be ushered in by the emerging vision for an internet of things (IoT), which will connect billions of objects – "things" like sensors, monitors and radio-frequency identification (RFID) devices – to the Internet. The scale of an IoT could far outstrip use of the Internet as we have come to know it and have enormous social and economic implications. There are <10 billion people on the planet, but estimates range from 50 billion Internet-enabled devices by 2020 (OECD, 2012) to a trillion in the longer term. Can they be put to work for digital economies around the world?

To bring the ensemble of technical innovations to work for digital economies and societies, policymakers, technologists and opinion formers need to understand the social and policy challenges raised by the varied uses of the IoT. If the right practices, policies and business models are developed, the IoT is likely to stimulate major social, economic and service

DOI 10.1108/info-09-2013-0047

innovations in the coming years and decades of its development. One forecast links the application of the IoT in manufacturing to a “fourth” industrial revolution, or what has been called “Industry 4.0” (Löffler and Tschiesner, 2013). And networked digital economies could harvest the potential of this wave of IoT innovation for a wide range of sectors, not only for manufacturing. It could become a ubiquitous feature of everyday life and work (ITU, 2005).

However, the future of the IoT is far from inevitable. Technical possibilities will not lead inexorably to successful public and private infrastructures that support everyday life and work. In fact, the IoT could undermine such core values as privacy, equality, trust and individual choice, if not designed, implemented and governed in appropriate ways.

The Internet has been reshaping how we access information, people, services and technologies, reconfiguring the way we do things (Dutton, 1999). The IoT will build on such transformations by embedding tags, sensors and actuators in objects that are networked through an open standard Internet protocol, phones, cars, shipping containers and more will no longer be simply physical objects. They will carry more information with them and become information and communication technologies as well as physical objects. In the coming decades, these devices are expected to be components of major infrastructures of smart cities, intelligent energy services, transportation networks, logistics, health and medical care services, households and other areas, including major applications in entertainment and the creative industries. The relevance of the IoT spans the entire range of networked economies and societies. However, they will require social and organizational innovations, but also innovation in information and communications policy and regulation, such as around privacy, data protection and intellectual property rights (IPR).

Research centres in many nations have embarked on initiatives to foster the development of the IoT. Early innovation of the IoT has been credited to MIT’s Auto-ID Lab, which was focused on the electronic identification of objects (Chaouchi, 2010). But decades ago, Singapore created a National Computer Board that fostered a vision of an “Intelligent Island”, which led to developments such as enabling every journey of every user of the city’s mass rapid transit network to be tracked, analyzed and visualized, and the data used to reshape the allocation of services to reduce delays and overcrowding (Choo, 1997). More recently, China launched an aggressive strategy to develop smart cities (Kortuem, 2013)[1]. The race to be first in deploying the IoT needs to shift to an emphasis on the most appropriate policies and practices to realize the anticipated benefits, avoid predictable and unintended social and economic risks from the earliest possible stages and balance conflicting values and interests in designing the IoT within all sectors.

The new IoT?

Throughout its first 40 years, the Internet has been used primarily to connect people with other people, such as through email, forums and, increasingly, through social networking sites (SNS); with text, such as over the World Wide Web; and increasingly with data, such as has been advocated in visions of open linked data (Berners-Lee and O’Hara, 2013). In the future, the Internet is also likely to be increasingly used to link devices, machines and other objects, or – in the vernacular – things, over wired and wireless networks using an open standard Internet protocol. This is not an entirely new phenomenon (Chaouchi, 2010). Ashton (2009) used the phrase “Internet of Things” as early as 1999. However, the scale, application and sophistication of this emerging ensemble of technologies are sufficient to view it as a genuinely new trend in emerging applications of the Internet.

The IoT captures the many permutations of detecting, tagging or identifying “things”, such as through RFID, bar codes, quick response (QR) codes, sensors and actuators, over the Internet and Web for such purposes as identifying, monitoring, sensing or actuating other devices that are online. This set of technologies enables products or other physical objects to store, send or receive information in ways that could transform the way we do things and justify this new concept – the IoT or Web of Things. In manufacturing, for example, it has been identified as the basis for a fourth industrial revolution or "industry 4.0", such as by enabling major advances in just-in-time lean manufacturing (Löffler and Tschiesner, 2013).

The IoT has been defined as "Internet-enabled applications based on physical objects and the environment seamlessly integrating into the information network" (IoT, 2013, p. 1). This definition represents a broad ideal, as many large-scale technological developments are not always seamless or integrated or functional. Also, the IoT is an umbrella term that incorporates a variety of more specific developments, such as sensor networks and machine-to-machine (M2M) communication. Some have argued for the use of more specific terminology, such as M2M (OECD, 2012), but such narrower definitions are tied to only a limited range of configurations of the IoT. Broadly defined, the IoT consists of the protocols and related technologies that enable these many different devices to communicate over electronic communication channels, wired or wireless – a network of things, including people, that some have called the "thingternet" (Valéry, 2012). The IoT enables electronic information to be transmitted by physical objects, such as when they move through space, in ways analogous to how wired and wireless networks convey electronic signals – creating a genuinely new dimension to the design and use of the Internet.

Applications across settings of use: an electronic chameleon

The IoT is most often discussed in the abstract, as a generic technical innovation. Technically, sensors and actuators are some of the basic building blocks of such IoT networks (Dutton *et al*., 2013). Sensors are built to detect a specific physical change, and only this programmed change, and convert that event to one that can be read by an observer or another electronic instrument. For instance, sensors recognize a finger pressing a button, a person approaching a door or entering a room. Actuators move or control a machine or system in response to a signal in ways that make a pre-specified change. Actuators are the associated devices that control a mechanism, such as opening a door, turning on a light or sending a message. Actuators that are embedded in a public environment or that can act at a distance may affect people other than their owners, such as by setting off an alarm. But the IoT becomes concrete and takes on many different shapes when placed in a specific social, organizational or environmental setting. Take three very different social settings of use: ecological sensing, the household and healthcare.

These three settings are among those that became a focus of one of the early large research and development efforts with sensor networks developed by the Center for Embedded Networked Sensing (Box 1). Consider the different issues tied to monitoring pollution in a waterway vs watching people in a public square vs remotely monitoring a person's heart rate or other vital signs. Given the variety of issues that arise in different settings of use and application, most discussions of the business models, technologies and governance issues involved with the IoT must move to a specific setting of use and application to be practical and useful.

Box 1. Center for embedded networked sensing

Center for embedded networked sensing was launched in 2001 at the University of California Los Angeles through funding from the US National Science Foundation and ran until 2011. This research group experimented with applications of sensor and actuator networks in such areas as monitoring the ecological environment, urban life and personal health. The issues involved in designing, installing, using and governing sensor and actuator networks in these different contexts are very different.

Adapted from: http://research.cens.ucla.edu/

It is, therefore, useful to see the IoT through examples, as they make the concept concrete and enable people to see its potential for application across a wide variety of settings. Table I provides a set of illustrative and by no means comprehensive set of examples of applications using a diversity of devices in different social and organizational settings that entail different sets of service providers, and third parties who might use data generated by the basic services. It is by linking together arrays of these technologies that more long-term visions have emerged for intelligent cities, transportation networks, manufacturing and households.

The Internet itself began as a means of networking computers to share distributed computing resources. A set of open standard protocols was created to network these machines, so the Internet infrastructure itself can be viewed as a network of networks or essentially an IoT. That being said, some of the early uses of the Internet linked people to things. In the UK, one early application was simply linking to devices for remote observation, including playful applications, such as looking at a shared coffee pot from one's office, but also serious applications, such as enabling robotic use of a remote telescope (Box 2). In more mundane applications, many Internet users routinely link to remote webcams, for example, to check traffic on their route to work or monitor their homes or offices (Box 3).

Another early use of telecommunications and computing has been to track and identify objects, such as to locate a stolen car. In this respect, some have argued that the IoT is simply an "expansion of traditional telematics, security and asset control applications" like the homing device used in the popular motion picture *No Country for Old Men* (Brisbourne, 2013). However, if Internet-enabled, one might home in on a device from anywhere in the world. More importantly, these devices will be capable of storing, receiving and sending electronic information when there is a change in their environment, or as they move through space, making them ICTs and not simply physical objects in ways that could transform the management of households, logistics, cities and more.

Table I Illustrative applications and actors in IoT services

Type of application	*Device*	*Setting of use*	*Network*	*Service provider*	*Third-party data users*
Monitoring and managing energy use	Smart energy meter reading	Household	Wired, powerline communication (PLC)	Energy providers	Government agencies, news
Remote monitoring, for diabetes, asthma, [. . .]	Sensor, webcam, microphone	Monitor wine cellar, childcare	Wireless mobile or wired Internet	Individual, Household	Other members of household
Environmental monitoring	Smartphone pollution apps	Pedestrian motorist	Wireless	Environmental NGO, researcher	Government agencies, press
Health monitoring	Smartphone app or email	Patient with particular diagnosis	Wireless	Health service, doctors	Insurance companies, pharmaceutical companies
Tracking	Tracking device	Stolen car owner	Wireless	LoJack	Insurance companies
Logistics management	Tracking device, GPS	Real-time tracking of freight	Wireless	SenseAware	Transportation planners, freight carriers
Manufacturing	Sensors, RFID	Lean manufacturing	Wired and Wireless	Manufacturers, suppliers	Customers, contractors
Quantitative self: running, jogging and personal data	Smartphone app	Individual in life and work	Wireless	RunKeeper, aggregators	Local governments, press, planners, other individuals
Location, travel directions	GPS navigation	Car, bike, pedestrian	Satellite and mobile wireless	Satellite navigation providers	Transportation planners, law enforcement

Box 2. Robotic Telescopes as an IoT

The first “effective” robotic telescope was developed in the early 1990s at the University of Bradford through support from the UK Particle Physics and Astronomy Research Council (Baruch, 2000, p. 119). Today, professional and amateur astronomers around the world can use the Internet to see through telescopes, illustrating the use of person to machine applications for science and education.

Box 3. Vint cerf’s wine cellar*

One of the fathers of the Internet, Vint Cerf, has enjoyed speaking about his ability to monitor the temperature of his wine cellar from anywhere in the world through a commercial IPv6 wireless network in his household. It monitors heating and cooling throughout the house and receives an alert on his mobile if the wine cellar gets too warm.

*Adapted from presentations, and: www.youtube.com/watch?v=EGSsjOynXg4

Mobile phones are equipped with sensors, global positioning systems (GPS) and the electronics to identify their location. This enables you to know where you are, get directions or find your children or a friend, anywhere in the world that a signal can reach, even if they cannot answer a phone or don’t know exactly where they are to tell you on a mobile phone. Other technologies, such as RFID, allow objects to be tagged at low cost in ways that enable the transfer of the data necessary to identify and track the object, such as when implanted in a pet to help identify its owner if it goes missing or placed inside a package to track freight in real-time.

Sensors and sensor networks are becoming commonplace. A sensor might be used to turn on the lights when you enter a room or set off an alarm if someone leaves a shop with an item they have not purchased. Yet the growing use of sensors to monitor the environment, such as those embedded in rivers and waterways to monitor pollution or through mobile phone environmental applications employed by users, enables real-time data that would have been unfeasible to collect and process before the cost of the technology dramatically declined (Bird, 2012). Estimates of the number of sensors that will be planted around the world are in the tens of billions.

The IoT is not just RFID, sensor networks or only M2M communication or just remote links to devices, but all of these ensembles and more that enable new devices to be connected with other devices and people in ways that provide applications and services that are new in their scale, geography and sophistication, often by being linked to capabilities in big data analytics (Table I). As discussed in the following sections, the IoT creates a new vision, new settings of use, new ways of doing things, new social and ethical risks and new governance challenges. Critically, however, all of these innovations must be considered across all the many and varied settings of use.

Is the IoT new and innovative?

Despite these distinctive aspects of the IoT, there is a continuing debate over whether this is a genuinely new development. Are business and industry simply trying to promote something as the “new new thing” (Lewis, 2000) or is it a serious departure from past technological systems? As noted above, components of this technology, such as the Internet and various components, such as sensors and devices such as identification technologies, like RFID, are relatively mature technologies, albeit constantly and rapidly evolving and being combined in new ways. Nevertheless, it is an emerging technology in several respects.

A new vision

The IoT presents a new way to think about the key areas for targeted innovation around the Internet. The concept of social media has focused more attention on SNS and applications, such as Facebook and its competitors. The Semantic Web, advocated by Sir Tim Berners-Lee, has focused more development around what he increasingly refers to as the Web of Linked Data (O'Hara and Hall, 2013, pp. 56-58), such as in underpinning support for the UK's Open Data Institute[2]. Social media, such as Facebook applications, use M2M communication to keep track of their users, and the IoT could feed the "big data beast", including the creation of open linked data sets, but it is a distinctly different vision from these related but more conventional applications of the Internet.

The IoT redirects attention from the development of applications focused on connecting people with one another, such as via electronic messaging and conferencing, what can be called "person to person". Nor is it focused on the development of linking people with texts over the Web or open data resources, or "person to thing". The IoT is more focused on putting devices online that are linked with other devices in person-to-machine, machine-to-person, machine-to-machine (M2M) or thing-to-thing networks. Of course, these IoT are often embedded in systems that incorporate people in a larger technical system, such as in health monitoring of a person using sensors and the mobile phone as a platform for networking with healthcare providers. The power of this vision is evident in the rise of entirely new programmes within business and industry, such as around lean manufacturing, smart cities, smart transport, smart homes and in other areas, as discussed below. In fact, some pundits have argued that the IoT is the biggest innovation in communication since the Web (Valéry, 2012).

New and diverse settings of use

The Internet can change the social dynamics of sensor networks and related networks of things. What could be a local homing device, requiring a sensor to be close to the homing signal to register it, could become global if Internet-enabled. An "old" example, the Active Badge System (Harter *et al.*, 2002), illustrates this point (Box 4). The geography of tracking (an employee, a person such as a prisoner on a release scheme, a car, a citizen, a shipping container or a consumer) is reconfigured if embedded in a global, Internet-enabled network of things. Closed and local networks can be opened and expanded online in ways that radically reshape the social dynamics of use, and, therefore, the potential uses and implications of the technology. Likewise, as discussed above, the social setting varies dramatically across applications. The use of the IoT for environmental sensing has a different array of actors and issues as stake than the remote monitoring of patients.

New ways of doing things: the social and organizational impact

As information and communication technologies (ICTs) reconfigure access to information, people, services and other technologies, they can transform how we do what we do, and

Box 4. The Active Badge System

Developed between 1989 and 1990 by Andy Harper and others, the Active Badge System used infrared signals in a cellular network to identify and track badges worn by people as a means of knowing their location and following their movements. The largest prototype deployment was at the Cambridge University Computer Laboratory. Andy Hooper and his colleagues could look on their network to see where people were located and see how this affected behaviour, such as not calling people who were out of their offices. Futuristic in 1990, it sounds quaint in the era of smart mobile phones. The team also focused on using a person's location to bring services to them, allowing applications such as documents they were working on to move with them, for example by transferring a file from the office to someone's home by following the person's location. Again, the need for such an application has been overtaken by such developments as cloud-based services, but the system was heuristically rich in generating new ideas about applications and services. Hooper's team also placed this data on the Internet so that members of the team from anywhere in the world could see where all the active badge wearers were at any given moment. In this specific example, the Internet changed the context of use, making it global rather than local.

the outcome of those activities (Dutton, 1999, 2005). This change can be incremental or more transformative (BCS, 2013; Dutton *et al.*, 2013).

Incrementally, libraries have experimented with better ways to check out books and to shelve them on return, and find them if shelved incorrectly (Box 5). Just as a car rental company can track its cars through GPS, more providers are likely to track more and more physical objects through GPS as their cost continues to decline. The tracing of freight containers, rail cars, and packages sent through the post, and individual items could be one of the key applications of the IoT. A more transformative example emanates from the "quantified self" movement (Box 6).

Related innovations spring from work on personal digital assistants or "digital companions" that learn about their users and provide advice and directions throughout the day (Wilks, 2007). Often supporting person–machine communication, these devices could also communicate with other devices, companions (Box 7). The development of devices sometimes called "digital companions" or conversational machines, is not new, but growing in their sophistication, such as in application of artificial intelligence such as based on language processing. They have been popularized by the feature film directed and produced by Spike Jonze, *Her* (2013), in which a man falls in love with his digital companion. The exact nature of the devices are uncertain with innovations such as MIT's

Box 5. The IoT in libraries

Barcodes and RFID have been used to enable a library user to check out a book simply by scanning a QR code on a library application on their smartphone, eliminating the need for staff to complete manual operations. This not only automates the library's work, but also "informates" the library (Zuboff, 1988), providing new forms of data for analyzing and visualizing the users of the library and their reading interests. Nevertheless, even such incremental changes could confront resistance from users if the IoT changes the role of library staff, such as reducing interactions with users, or creating a sense of greater surveillance in the workplace and everyday life (Boos, 2013).

Box 6. The quantified-self movement

Individuals within this growing community enjoy using technologies to monitor their behaviour, such as their running, sleeping or eating patterns, in ways that provide instant feedback and enable them to better manage their lives, often by making social comparisons with others. A blog for this community is subtitled "self knowledge through numbers" (http://quantifiedself.com/). Of course, many people have long kept track of their behaviour, such as through diaries, but this is an example of a quantitative change that can make a qualitative difference. Simply by keeping a tracking device on your wrist or clipped to your clothing, sensors can, more or less, accurately detect how far your run, how well you sleep and more. In addition, social comparisons can be done without individuals sharing information face to face or even knowing each other, making this a qualitatively different experience. However, quantitative self-applications do not prevent the sharing of information within a close social circle, where there can be additional social support to reinforce the achievement of behavioural targets.

Box 7. Digital companions

A digital companion could speak through an avatar on your mobile phone or personal computer or any other device and move seamlessly across them. It could remind you of appointments, which pill to take, how to contact a friend, give directions and so on, much like smartphones and tablets can in more rudimentary forms (Wilks, 2010). It will be a "smartphone on steroids", of particular value to those without the ability or wish to use a touch screen or keyboard. It will know and learn a great deal about its user, and, therefore, need to be governed by rules, or else be allowed to reveal and disclose anything about its user, such as to another person's companion. An "anything goes" strategy might be appropriate in early experimental phases but be inappropriate as the devices become more ubiquitous and capable of increasingly sophisticated communication.

Pattie Maes' "SixthSense"[3], Google Glass and the digital companions presenting different possibilities.

Another transformative example within institutions comes from healthcare. If the monitoring of a person's health progresses through the use of systems for tracking a person's condition, the delivery of health services could be fundamentally changed (Box 8). Imagine a future in which patients can move beyond searching for information online to manage their own healthcare or no longer call or visit their doctor or hospital when they feel ill or notice a medical problem. Instead, before they even feel ill or are aware of a symptom, they could be called by their healthcare provider and told that they should come in, that the provider has been monitoring them and noticed something that should be explored further. Of course, the concept of a doctor calling you, rather than vice versa could be and has been extended to any number of services, from car repair to banking, and this is a business model that is already developing, such as when we get a car checked when warning lights indicate a problem, rather than waiting until things breakdown. Again, however, this could be fine-tuned and applied to many services in transformational ways if the right technical and business models and governance can be put in place. No pushing buttons. Things happen when needed and in response to conditions or events as they occur.

Features of a new technology

There are a number of characteristics the IoT that underpin its significance.

First, it is very flexible given the generic building blocks of the IoT, such as sensors and actuators that can be combined in many ways and applied in diverse contexts. Moreover, each component, such as sensors and RFID, are being constantly progressed in ways that open up new areas of potential application. The same technologies that can enable lean manufacturing, permitting manufacturers to minimize their inventories and track needed parts and components worldwide in real-time, can be brought to bear on the management of cities or transportation networks to enhance the efficient use of scarce resources.

Second, the IoT does not always do something entirely new, but does things closer to real-time and at a greater level of precision than has been done before. For example, many applications tied to "smart cities" envision applications such as improving police manpower allocation by harvesting increasingly up-to-date and precise data about crime patterns and police presence over time and across the geography of a city. Police manpower allocation has been supported by computing for decades, but with the IoT feeding into sophisticated big data analytics, crime patterns could be tracked in real-time and linked with other sensor

Box 8. Remote patient health monitoring

Gari Clifford in the Robotics Group at Oxford University's Department of Engineering Science has been experimenting with the implementation of a variety of health-monitoring networks built around simple tools, such as the mobile cellular phone networks and the Internet. He calls this "Intelligent Patient Monitoring and Signal Processing/Data Fusion", and conveys the vision of his group on his website:

> Our vision is to provide an open-source customizable medical data exchange platform which, amongst other things, allows the collection of accurate labelled medical data. Not only does this facilitate low-cost diagnostics and treatments, it also allows us to develop intelligent agents to perform automated quality control and decision support. The hope is that the use of artificial intelligence on personal devices, trained on an ever expanding ark of patient- and disease-specific medical data, will expand distributed diagnostic care from millions of healthcare workers to billions of individuals. In this way we may provide low-cost personalized medicine which patients manage themselves[4].

He has experimented with a wide range of health issues, from remotely tracking a person's heart through an electrocardiogram (ECG) to tracking a person's psychological state.

data on a wider geographical scale that would allow analysts to redeploy police on a continuing basis and adjusted in real-time to respond to shifts in crime and conditions.

Third, data sharing is a key aspect of the IoT. Discussion of the smart city emphasizes the need to integrate data across different sectors and services, such as sharing real-time data on energy use (Box 9) or transportation, not only across different transportation systems, such as between metro, bus, rail and vehicular traffic but also with other sectors, such as with environmental sensors. Already, environmental applications on mobile phones in China have been valuable in monitoring pollution levels, creating a new source of information that is more independent from government (Hook, 2013). Such aggregated data could shape the behaviour of pedestrians, such as not exercising when pollution is at a high level or staying indoors. The idea of sharing data collected for one purpose to support another is fraught with new issues of policy and practice, but the idea of sharing is central to enabling the IoT to be more capable of supporting applications that entail knowledge of behaviour. Combining data about different individuals can be of great value, just as the Web has shown that distributed individuals can collaborate in ways that create new forms of collective intelligence.

Legal, ethical and social risks

It is difficult to consider these potential transformative applications of services without bumping up against the ethical, legal and other social risks they entail, for example, when tracking and monitoring a person's whereabouts, much less when following indicators of the condition of their health, such as a patient's ECG or their psychological state. The most central and apparent risk concerns compromising an individual's personal privacy, creating systems that would make data protection ever more critical under existing law and policy.

In the 1990s, when I described the Active Badge System (Box 4) to students, they were uniformly concerned over the implications of employers tracking employees. In the 21 century, mobile phones with various applications that rely on tracking location to give directions or find a friend have raised related concerns over access to location and other personal data by public or private actors who do not have permission from or the consent of the user. At other times, they are taken as a useful service, such as in meeting people. Internet service providers and search companies are under increasing scrutiny over whether they are passing on data about their customers without the informed consent of their users. That said, similar concerns were raised over electronic banking and funds transfer systems (Kling, 1978), but banking and payment systems have developed policies and practices that have won the trust of most customers. But privacy and surveillance are among an array of social and ethical risks tied to the IoT (Spiekermann, 2013). Other issues are ownership and IPR, security, systemic failures, social isolation, disempowerment of individuals and inequities across digital divides.

Members of the public are watched increasingly by cameras and sensors, and the IoT is likely to extend the potential for electronic surveillance in new areas (Weber, 2010). The technology behind efforts to resurrect a national identity card in Britain was anchored in developments around the IoT, enabling the creation of unique electronic identifiers for the cards, a development that raised major privacy, data protection and security concerns.

Box 9. Personal monitoring through smart energy meters

A simple example of sharing is the possibility of using data gathered from monitoring smart energy meters in households to automatically identify a potential problem, such as appliances that might be left on or faulty. More unanticipated applications are also possible, such as detecting whether an elderly person has not gotten out of bed for their morning cup of tea. If so, should an actuator ring a family member's mobile phone?

Privacy issues are difficult to solve without raising other issues, such as over trust. There is a "trust tension" tied to privacy, as explained by Guerra *et al.* (2003, p. 3) in noting that:

> [. . .] data collection can help trust by creating a legal bond between the parties involved. However, the collection and availability of data can create problems of trust in terms of privacy because individuals may be wary of data surveillance, or of the secondary use of that information. Indeed, privacy is repeatedly identified as a concern that prevents consumers from using the Internet for transactions. In this way, there is a "trust tension" between privacy and identity: absence of data impedes trust as accountability is limited, but data gathering creates trust problems regarding the use of the data [. . .] and intrusions on privacy.

In generating data about individuals, the IoT will create concerns over privacy, while the lack of data would also undermine trust. Balancing these tensions will be a key aspect of any service or offering, much like social networking services try to balance concern over privacy by seeking to ensure that users have control over their privacy settings.

These issues are closely tied to uncertainties over ownership and control.

Who owns the data collected by the IoT in various contexts that involve multiple actors, such as patients, doctors, hospitals and others, in the case of patient care? In many contexts, copyright agreements are likely to assign ownership of data produced by a machine, such as a sensor network, to the controller of the machine. Open systems might jeopardize the controller's ownership and control of that data, creating an incentive for more proprietary networks. On social media, for example, a user of a social network site does not yet have the right to transfer their data to another service provider, as their social network provider owns their data, and a user's network involves the data of other users. Similarly, in some contexts, ownership is contested, such as with health data, when patients, hospitals and data controllers might all have a claim to ownership, such as of a medical image or genomic data (Dutton and Piper, 2010; Kay, 2010). As data generated by an IoT becomes more central and is shared across sectors and applications, this issue will become increasingly important and more complex.

The possibility of theft or other unauthorized access to the data or systems developed around the IoT means that cyber security needs to be another priority for reliable systems. The IoT could generate highly sensitive personal data as well as supporting safety critical systems, such as in managing power or transport, or monitoring human physiology, for example, with heart pacemakers. These systems need to be secure from natural disasters, intrusion by any unauthorized users or accidental data breaches by well-intentioned personnel authorized to handle data. A far-fetched fictional portrayal of a Vice President assassinated through remote control of a pacemaker created an entertaining episode of the American television series *Homeland*, as early security flaws in the wireless transmitters used to send instructions to heart pacemakers made it technically possible to deliver a deadly shock (Kirk, 2012).

A related fear is over the development of systems that could create greater potential for large-scale failures.

Will the IoT create more highly coupled organizational and service delivery systems that remove human intervention and could be more prone to system-wide failures or crashes, a concern that has been raised about computerization, in general (Rochlin, 1997; Head, 2014)? Take the example of an unruly actuator in a tightly coupled system[5]. There is a risk of people being adversely affected by actuators that are not correctly set or are maliciously set, or subject to adverse interactions between different actuators, as well as through simple malfunctions and programming mistakes (Box 10). In such cases, it may be difficult to diagnose or correct the problem locally. All these concerns are compounded by the potential for the Internet and Web to be scalable enough to handle a trillion things in a reliable way to support safety critical systems that the Internet was not originally designed to support (Zittrain, 2013).

Box 10. The public lavatory calling

There has been a graphic case of a person being repeatedly telephoned by a public lavatory that ran out of supplies. It was programmed with the wrong number for contacting the supplier. Who does one call? It is likely to be very difficult to correct such a mistake.

See: this actually occurred in 1997: http://catless.ncl.ac.uk/Risks/19.33.html#subj1

The potential for taking human beings out of management and service delivery is another threat of the IoT. Despite journalistic coverage to the contrary, networked individuals are more likely to have social relationships with family and friends than those offline, who are more likely to be isolated (Rice *et al.*, 2007). However, the IoT could change this pattern. The IoT primarily provides commercial services, but in the provision of such services, people will be increasingly connected with things in ways that could potentially isolate or distance them from other people. We will fill out more templates on electronic pre-set forms. We send email to and receive email from software programmes. Just as it is increasingly difficult to speak with a live person on the phone, as opposed to an automated message system, so the IoT might transform the Internet into an increasingly inhuman artificial society. Robert Redford, in the popular feature film *All Is Lost*, is left stranded as a high-tech container ship passes by without any person for him to reach.

This is explained as an issue of cost savings, enabling a few unskilled information workers to handle systems that can scale to thousands or millions of users. Would you rather have a grandparent watched by a sensor network to alert you to a problem, or not watched at all? Ironically, perhaps, in the age of an IoT, it will cost more to speak or interact with a human being. The digital divide could flip around, with those less well-to-do managed by things and those more well-to-do able to deal with people. This is not a technically determined outcome, but one that will be driven by social and economic choices in the years ahead. The IoT could, indeed, enhance human interaction, such as by enabling more social support for older people in homes and care centres that could increase contact with family and friends. Research needs to track the social impact of the IoT in this and other areas.

A closely related issue is over the *locus* of choice in an IoT. Will the IoT empower individuals who seek to benefit from the services or centralize access to information and control in ways that empower institutions and undermine the customer? Smart energy meters could permit individuals to self-regulate their energy use in ways that save money and energy. But if individuals fail to regulate their use, will energy companies intervene, for example, by not permitting an appliance to be turned on at particular times? Smart transportation could enable drivers to avoid congestion and drive more efficiently, but also be used by governments to implement road pricing and manage traffic through charging policies that could constrain user choice. Driverless cars are one logical extension of this trend toward removing control from the user. In the near-term, data about drivers could be used by insurance companies to price policies in ways that drivers might well resist.

The IoT is usually discussed as a “ubiquitous” technology, universally available to all (ITU, 2005), but it is most likely – as with most technological services – to be unevenly distributed in ways that follow and reinforce existing digital divides. For example, those who have multiple devices for accessing and using the Internet – so-called “next generation users” – tend to be people with higher incomes (Dutton and Blank, 2011, 2013). This is not to say that the IoT is uniquely poised to exacerbate inequities, but it is often spoken of as if equally available to all. There is no doubt that the mobile smartphone will bring many of the next 2 billion Internet users online, but smartphones and other portable computing devices and applications in Britain and other developed nations are most often purchased by people who have one or more computers in the household and workplace, adding to other devices such as tablets and readers and deepening divides between those without access and the Internet-enabled users.

Globally, the IoT could exacerbate inequalities in economic development across nations and regions, although many areas in the rapidly developing world, such as in China and East Asia, are a focus for IoT activities, in part because they are building new infrastructures, rather than retrofitting old infrastructures such as enabling wireless access on the London Underground. Yet it is likely that the IoT will be more prominent in the wealthier nations of the world and reinforce global digital divides.

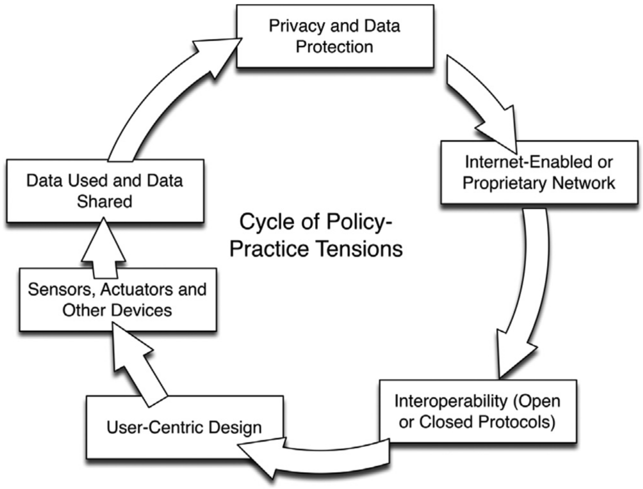
New governance challenges

Given all these new aspects of the IoT, it will present major issues of governance – policies and practices adequate to control and manage the IoT across a wide variety of contexts. It is one thing to develop appropriate policy and practices to govern the Internet and Web, although this continues to evade most national and international forums, but the IoT will involve a much greater scale of connections. Since the IoT can be used in many contexts to collect data that separately or in combination with other data can generate sensitive personal information, it promises to increase the number and range of issues tied to privacy and data protection, as but one example. Moreover, given the centrality of data-sharing across applications and sectors, issues of privacy and data protection will be especially difficult to manage, as the ecology of actors will differ across each setting of use, as illustrated in Table I. There is likely a growing tension between privacy and other values touched by the IoT (Guerra *et al.*, 2003; Dutton *et al.*, 2005). Figure 1 illustrates the potential tensions between various values at stake in the design of the IoT, such as between privacy and data sharing.

As Figure 1 suggests, a focus on user-centric design can lead to the design of an IoT using sensors and other devices to provide more data that can be shared across applications. However, if this leads to concerns over privacy and data protection, this could push providers towards more closed proprietary networks rather than open Internet standard protocols that might undermine sharing and more user-centric designs. How to balance these concerns and avoid a vicious cycle of policy–practice tensions undermining the value of the IoT is a key issue for the future of the IoT.

There will be a host of other IoT policy issues that need to be resolved that can only be briefly noted here. These include:

Figure 1 Cycle of policy–practice tensions


Privacy and Data Protection
Internet-Enabled or Proprietary Network
Interoperability (Open or Closed Protocols)
User-Centric Design
Sensors, Actuators and Other Devices
Data Used and Data Shared
Cycle of Policy-Practice Tensions

Source: Author

- *Open vs closed systems.* Will networks develop as a multitude of proprietary systems or a more integrated Internet-enabled ecosystem built on open standards (Ziegler *et al.*, 2013). Alternatively, there could be a complex mix of closed and open systems.
- *Spectrum management.* While the bandwidth demands of the IoT, such as with M2M communication, should be far lower than voice and video communication, there are continuing spectrum issues for mobile service providers, and the IoT will generate more demands for freeing spectrum for the IoT from other services or creating more unlicensed spectrum to prevent the degradation of signals and services (OECD, 2012, pp. 35-36).
- *Numbers and addresses.* The IoT could create an added incentive to move faster toward adoption of IPv6 protocols as a means of creating more addresses to support end-to-end connectivity (OECD, 2012; Ziegler *et al.*, 2013). Telephone numbers will also need to be increased because many devices require multiple numbers (OECD, 2012, p. 37).
- *Roaming.* The harmonization and pricing of the use of spectrum across local and international jurisdictions is already an issue for mobile and smartphone applications (OECD, 2012). While M2M roaming escapes the charges applied to mobile phone applications, M2M services will require continuing negotiations among carriers and regulators to enable global business models to support particular services.

These issues need to be dealt with at scale, with plans for sensor and related IoT devices to encompass up to a trillion connections[6]. This is a difference in scale that has major consequences for manufacturing devices, managing their deployment, implementation and use and governance.

The future of the IoT

There are at least four competing perspectives on the future significance and impact of the IoT: as being overly hyped, an economic imperative, an insurmountable opportunity or a useful vision. While all have some merit and adherents, this is a vision that has already provided useful guidance to business, industry and government and will become far more prominent in the coming decades.

Overly hyped

A significant component of commentary on the IoT argues that there have been useful applications of identification, tracking and sensing technologies, but that this area is not new, and most importantly, lacks a strong compelling business model in many cases. In other words, it is not yet viable and possibly not even around the proverbial corner (Valéry, 2012). One commentator draws the Gartner Hype Cycle to show that the IoT is on the upward trajectory of the cycle, suggesting that it has yet to reach the “peak of inflated expectations” before dropping to a more realistic level of expectation (Taylor, 2012). However, it is impossible to launch any new technology without some level of promotion. Elimination of all the hype could undermine its success. But it is critical that policymakers and managers realize the prominence of hype surrounding emerging technologies and make their own critical assessments of their value in their own particular contexts of use and impact.

Economic imperatives driving towards a predictable collision

A quite different scenario views the economic case driving the momentum behind the development of the IoT to be great and unstoppable. From this perspective, for the Internet or computing industry to dismiss the IoT would be folly, given that the scale of development and investment in this area is already huge and forecast to grow substantially. It is a new front for the digital economy. However, this “technology out of control” scenario will lead to an almost inevitable train wreck if the momentum behind the IoT is allowed to run into the very predictable privacy, data protection and other social issues tied to sensors, actuators, homing devices, identification technologies and more, being embedded in everyday life and work. To realize the economic pay-offs of the IoT, these social issues and value trade-offs need to be resolved early on in the design and development of systems.

Unrealised opportunity

Another scenario sees the opportunity behind the IoT as the logical next step for the technology, and the business case to be very positive in many areas, but impossible to achieve in practice. It is feasible technically and financially, but unlikely to overcome a number of organizational, institutional and public policy constraints. The IoT promises to change the way we do things, as discussed above, but organizations and institutions are slow to change. This social inertia will be further complicated by the serious issues facing the IoT in the policy arena, such as overcoming concerns over privacy and data protection, ownership and standard setting across jurisdictions. Interoperability is even a challenge within legal jurisdictions, given the use of proprietary networks and closed protocols. In this scenario, there is no train wreck, but developments will be slowed dramatically to allow social and policy change to catch up with technical opportunities. The degree to which nations are able to surmount these difficulties could depend on the structure of policymaking within each country. For example, it is less likely that more liberal democratic regimes would push forward rapidly with the IoT, given the range of issues surrounding their governance and use. Early developments in Singapore and China illustrate the value of more top-down decision-making, but the deliberation and pace of change in more liberal democratic nations could enhance the likelihood of a more acceptable and successful set of policies and practices in the longer run.

Useful vision for shaping innovation

A final vision that is the most realistic is that the IoT presents a very useful normative vision for how to develop a new phase of Internet applications and services. It is not an inevitable step, but it captures a growing trend in technical innovations, such as the rapidly declining costs of electronic devices, like RFID and sensors, giving it an increasingly strong business case; the declining cost and location-free access to storage space, such as through cloud computing services; and the major expansion of address space that can be created by such innovations as IPv6 (Valéry, 2012). A number of major players in the computing and Internet industries are investing heavily in this area, providing further evidence of early targets for application, and a viable business case[7].

It is possible to identify some clear areas of application that could be early targets for development, such as around the management of logistics or manufacturing, which address major concerns and have huge economic potential, summed up by the promise of a fourth industrial revolution (Löffler and Tschiesner, 2013). In addition, these areas are not as hyper-sensitive as such areas as health and medical monitoring that might well face the most difficult issues over ownership, privacy and data protection. Identifying these primary early areas of application will enable many of the most complex social and policy issues to be anticipated and addressed in advance of major investments. However, the challenges in areas such as health and medical monitoring should encourage research and development to focus early efforts to grapple with these issues to open them up to advances that could be ushered in by the IoT.

Uncertainties

Despite the value of this emerging vision for the IoT, there are major areas of uncertainty that could frustrate progress on the IoT.

Points of critical mass

Dramatic growth is most likely to occur once the IoT reaches a critical mass in its application within various sectors. Many demonstrations and an increasing number of applications have yet to reach a critical mass of providers and users, when further use will more rapidly diffuse. For example, quantified-self applications began to reach a critical mass only since 2010. Issues of standards, business models and the social and ethical issues tied to different areas of application begin to be resolved once a technology reaches this point.

Organizational and institutional innovation

Meaningful technological change involves an interaction between technical and organizational–institutional innovations. The technical infrastructures for an IoT might be available today, but the organizational and institutional infrastructures, including the skills, top management support and business processes are often more difficult to put in place because they involve social change. As noted above, the IoT should change how we do things, which means social and organizational change must accompany technical innovation. New forms of healthcare, enabled by an IoT, could be every bit as difficult as efforts to change the management or structure of national healthcare service delivery. That said, the IoT could enable and support innovations in organizational practices. Nevertheless, organizational and technical innovations need to co-evolve in supportive ways.

The complex ecology of actors shaping the IoT

The ambitious vision of smart cities and transport networks enabled by an IoT demands that their development bring together the full range of actors involved in the services and institutions that are affected either in the production, delivery, consumption or regulation of devices and services. This will entail collaboration across multiple regulatory agencies, industries and departments or ministries, making the ecology of actors difficult to even identify, much less to orchestrate to obtain a consensus on policy and practice. It is critical that early efforts to map the ecology of actors that are necessary to move forward on the IoT in different sectors be a high priority if they are to succeed. It may be equally important that steps forward on such visions as the smart city are incremental building blocks, which do not entail the full range of actors tied to the larger vision.

Need for an array of new business models

A number of the most successful Internet companies owe as much to their understanding of their underlying business models as to their technical acumen. For example, Google was not only a leader in search technology but also one of the first companies to see a business model in search. There are many developing business models for Internet businesses and services (Cusumano and Goeldi, 2013). The IoT is likely to both undermine old business models and require the further development of new business models specific to particular applications and sectors. In the foreseeable future, economic and financial constraints are likely to force governments and industries to depend on creative business models and not rely only on huge public infrastructure investments, particularly because these new services must be sustainable over the long term.

Policy issues that could kill the IoT

Policy issues could undermine the pace and significance of innovations around the IoT. Privacy is one of a number of issues, but one in which there is work in progress to address the issues in particular areas, such as in smart metering[8]. There is a clear need to create a set of policies and practices that will support the IoT in ways that do not undermine core values and ends that are critical to the larger economy and society, ranging from employment to human rights, so there is a need to anticipate such policy issues as early as possible in the design and development process.

Strategic settings of use

All these issues are further complicated by the degree to which the design and impact of the IoT will vary dramatically across different social settings of use, as discussed above. There is a limit to how far government and industry can advance the IoT without focusing on specific contexts, such as energy or healthcare. However, the most viable early wins for the IoT might be the more feasible applications, such as logistics, manufacturing and environmental sensing, that may not be the most attractive from the perspective of the policy community or the public, but which would have major economic payoffs and advance research and development on the IoT. Therefore, some hard social and policy choices involve the targeting of strategic settings of use for developing the IoT.

Key strengths, weaknesses, opportunities and threats

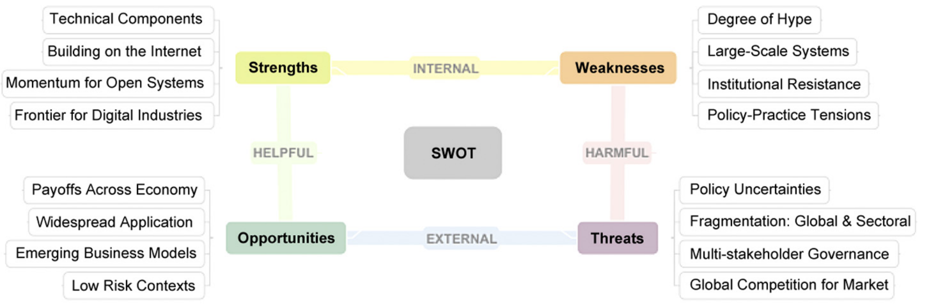
One way of capturing the complex array of factors shaping the success of the IoT is through a simplified high-level analysis of its strengths, weaknesses, opportunities and threats (SWOT) (Figure 2). As Figure 2 illustrates, key strengths are the growing capabilities of the building blocks of the IoT, such as sensors and RFID components. In addition, it builds on the success of the Internet and the momentum behind open standards, creating a genuinely new frontier for digital industries, which has already focused large-scale investments.

Despite the availability of all the components of the IoT, there are weaknesses tied to the hype surrounding a technology that involves large-scale technological systems, such as those that would be required for approaching visions of a smart city. It is also surrounded by hype that could undermine its credibility, and there is likely to be institutional resistance to the IoT, which promises to change the way people do things, requiring social and organizational change, not just technical innovation. Moreover, the policy–practice tensions (Figure 1) discussed around the IoT will require difficult balancing of the diverse values and interests of different stakeholders.

Nevertheless, the IoT presents huge opportunities, not only for digital industries but also for manufacturing industries and sectors across the entire economy that would gain from such pay-offs as more efficient transportation and energy use. Its potential application is widespread, hardly leaving any arena, from manufacturing to creative industries unaffected. Moreover, there are some emerging business models for supporting the IoT through cost savings, for example, in lean manufacturing, and some relatively low-risk contexts for its early development, such as in environmental sensing, rather than health monitoring.

Key threats include the uncertainties of public policies of relevance to the IoT, such as around privacy and data protection. Moreover, the large-scale systems that would be most valuable for an IoT could be fragmented by proprietary systems and closed standards that

Figure 2 A high-level SWOT overview of the IoT



Source: Author

vary within and across national jurisdictions. It will require multi-stakeholder governance structures at local and global levels, creating another threat to its success. But because the promise of the IoT is well-known globally, there will be major digital industry players competing for this new market, creating one of the greatest threats to those who only stand back and watch.

Summary and conclusions: directions for research

Much has been written about the technical design of an IoT, but it is far from simply a technical project. It is a major social development that could improve or undermine our quality of life, depending on the choices made over the coming years. Policymakers and practitioners need to marshal support at all levels to ensure the successful development of the IoT. To achieve this, they will need to:

- *Build public awareness.* Policymakers share a responsibility with academics, the media, business and industry to inform and foster public understanding of the IoT, for example, through providing clear information to non-technical readers and viewers, and fostering debate over the future application and implications of this innovation.
- *Build new business models.* Technologies are key to this new infrastructure, but so are the business models that will sustain it. Business and industry are likely to be creative in developing and evaluating business models, but academic research can help identify emerging models (Cusumano and Goeldi, 2013).
- *Foster openness to experimentation.* Nations and localities need to build a culture and setting that is more open to experimentation with and through pilot and demonstrator projects involving the IoT. This could entail the development of shared infrastructures for experimentation as a means of enabling small companies and enterprises, as well as creative individuals, to have access to infrastructures they might not otherwise be able to use for trialling technical innovations and new commercial or public services.
- *Enable multi-stakeholder approaches to governance.* Like the Internet generally, the IoT will be most valuable in a global network of networks, such as could be fostered through the development of open standards and protocols. This can only be accomplished by gaining the support of the full range of stakeholders in government, business, industry and civil society, not only in the UK but internationally.
- *Balance conflicting values and interests.* The IoT will be a major source of new forms of data about individuals, households and communities, and about society at large and its environment as sensors monitor rivers, public spaces and people in many contexts of use. It is critical that privacy and data protection, as well as related issues of IPR, ownership and consent are addressed early in the development of applications and services lest they put the brakes on the development of an IoT that is empowered by sharing of data across applications and sectors. Openness can conflict with other values and interests, such as privacy and data protection. Policies and practices in each area of application of the IoT must carefully balance contending interests.

This “new new” IoT raises issues and tensions, as its development and use will have major social and economic implications across many different settings of use (Lewis, 2000). Policymakers across all sectors of government and industry can help realize the potential of an IoT if they develop a personal understanding of the IoT, and its potential applications in many different contexts. They need to play a role in building public awareness of the technical, and also the social aspects of the IoT, such as by supporting excellent outreach from publicly targeted forums and reports to entertaining video productions and demonstrators of the IoT. Policymakers and practitioners need to anticipate key policies critical to the IoT in such areas as privacy and data protection, data sharing, provenance and ownership of data and open standards and protocols.

It could also be useful to create incentives for leaders to work together across industrial sectors and various contexts in which the IoT can be applied. There are profits to be made from the IoT, but a demonstrated potential for more radical innovation and more valuable applications could foster cross-industry collaboration, such as on issues of standards and open protocols to support greater interoperability. As underscored here, the IoT is not simply an information technology project. It will involve a commitment to investing the time and resources necessary to enable collaboration at all levels among health providers, transportation planners, logisticians, manufacturers, energy suppliers and in other application areas. Those who invest in the IoT in business, industry and academia should insist that research and development address predictable social, legal and ethical issues in the earliest stages of design and development, and not leave them for others to grapple with downstream[9].

The IoT represents a rapidly emerging technological vision for the Internet and related technologies, such as RFID, sensors and other electronic devices[10]. This vision moves from an emphasis on connecting people to one another and to documents and data, to connecting things – devices that can operate in systems with the aid of intelligent agents and people. Even though much of the IoT is not new, such as the development of sensor networks, the emerging vision entails connecting things at a new scale, sophistication and range of application and feeding into related developments such as around big data analytics and smart cities and transportation systems are innovative.

The IoT is likely to be of major significance to social and economic development worldwide. However, its development is likely to be constrained by social and organizational factors and public policy, as it brings up major legal and ethical issues and other problematic societal risks if they are not dealt with early in their development. There is, therefore, a need for early and anticipatory debate over the issues raised by the IoT in various contexts of use. Multi-disciplinary research on its development is critical, given the complexity and interactions among the technical, legal and social issues entailed in its use and implications.

Social science, along with other multi-disciplinary perspectives, should play a vital role early on in identifying and challenging assumptions about the design, implementation and impacts of IoT. Moreover, some of the social and economic implications – intended and unintended – are potentially issues that could undermine development or implementation. These issues need to be better understood at the earliest stages and in each particular setting of use.

The IoT brings new opportunities and threats to privacy and data protection, which are, therefore, critical to highlight within any IoT research agenda. These concerns are closely tied to related issues of open systems and could undermine efforts to develop an Internet-enabled network of things. The IoT carries with it an inherent assumption that information will be shared across applications and sectors to be most useful. Realizing this potential value of data sharing depends on resolving privacy and data protection issues, and related issues over informed consent to the use of data for a wide range of unanticipated purposes. Privacy and data protection are also related to issues of user-centricity, security, ownership, IPR and control, which will shape whether we use the IoT to create a network society that empowers individuals, or an artificial society that isolates individuals behind machines.

The IoT also brings with it a new, unprecedented scale of development, given the potential for a trillion Internet-enabled devices in the foreseeable future. However, there appears to be a lack of appreciation of the scale and the possible pervasiveness of its potential application across all sectors of society. Regulatory processes designed to cope with hundreds or thousands of transactions or services might need to be reconsidered to cope with a Web of a trillion "things" and the data they produce. New developments around the IoT will move faster than law and policy, creating an almost certain crisis of governance and policy in this area unless they are addressed urgently. Some of the key issues of governance and regulation include accountability for failures and data breaches, determining who sets standards, rethinking data protection policy and effecting institutional changes to cope with the scale of the IoT and its applications.

Many technological, organizational, cultural and regulatory infrastructures need to be put into place before the IoT will transform industrial and societal processes and services. This realization drives a need for inter-disciplinary research on the social and institutional shaping and governance of the IoT and its societal implications. There is a need to support interdisciplinary research programmes that focus on the technical, economic and social factors shaping innovations around the IoT, such as public trust in these new infrastructures and services, and their social and economic uses and implications (IoT, 2013). Yet academic research must be accompanied by collaboration across business, industry and academia on technologies and standards could foster innovation, while avoiding each sector reinventing the IoT in parallel rather than in collaboration.

Notes

1. www.china.org.cn/china/2012-12/07/content_27339102.htm
2. www.theodi.org/about
3. www.ted.com/talks/pattie_maes_demos_the_sixth_sense.html
4. www.robots.ox.ac.uk/~gari/
5. Miranda Mowbray of HP Labs brought this out in Dutton *et al.* (2013).
6. www.hp.com/hpinfo/newsroom/press/2009/091105xa.html
7. For example, IBM has championed developments around smart cities and related applications for years, and Cisco, HP, and others have made huge investments. See http://www-935.ibm.com/services/us/gbs/bus/html/smarter-cities.html
8. www.ffw.com/publications/all/articles/smart-meters.aspx
9. In the UK, for example, the Technology Strategy Board's (TSB) Connected Digital Economy Catapult (CDEC) has identified the IoT as one of its strategic priorities, providing government and industry with an opportunity to stimulate industry-led research, development and implementation across areas of application.
10. This vision is nicely conveyed by a cartoon-like but accessible IBM video: www.youtube.com/watch?v=sfEbMV295Kk

References

Ashton, K. (2009), "That 'Internet of Things' Thing", *RFID Journal*, available at: www.rfidjournal.com/articles/view?4986 (accessed 22 June).

Baruch, J.E.F. (2000), "The future of robotic telescopes for education", *Publication of the Astronomical Society of Australia*, Vol. 17, No. 2, pp. 119-124.

BCS (British Computer Society) (2013), "The impact of things", *ITNOW*, pp. 6-9.

Berners-Lee, T. and O'Hara, K. (2013), "The read-write linked data web", *Philosophical Transactions of the Royal Society*, Vol. 371: 20120513, available at: http://dx.doi.org/10.1098/rsta.2012.0513 (accessed 25 June 2013).

Bird, J. (2012), "M2M communications: 'internet of things' breaks through $10 barrier", *Financial Times*, 24 February.

Boos, D. (2013), "Transformation of society", abstracted in BCS, pp. 6-7.

Brisbourne, A. (2013), "The internet of things isn't as new as it seems", *Forbes*, CIO Network, available at: www.forbes.com/sites/ciocentral/2013/02/08/the-internet-of-things-isnt-as-new-as-it-seems/ (accessed 20 February 2013).

Chaouchi, H. (Ed) (2010), *The Internet of Things: Connecting Objects to the Web*, John Wiley & Sons, Hoboken, NJ.

Choo, C.W. (1997), "IT2000: Singapore's vision of an intelligent island", in Droege, P. (Ed), *Intelligent Environments*, North-Holland, Amsterdam, pp. 49-65, North-Holland, Amsterdam.

Cusumano, M.A. and Goeldi, A. (2013), "New businesses and new business models", in Dutton, W.H. (Ed), *The Oxford Handbook of Internet Studies*, Oxford University Press, Oxford, pp. 239-261.

Dutton, B., with Capra, L., Ciaraldi, M., Evans, D.F., Furness, A., Graham, I., Jirotka, M., Kupai, A., Maguire, M., Matthews, N., Mowbray, M., Payne, M., Prendiville, A., Steinmueller, E. and Tyrrell, R. (2013), *A Roadmap for Internet of Things: Social Sciences*, TSB Special Interest Group on the Internet of Things, Technology Strategy Board, London.

Dutton, W.H. (1999), *Society on the Line*, Oxford University Press, Oxford.

Dutton, W.H. (2005), "The internet and social transformation: reconfiguring access", in Dutton, W.H., Kahin, B., O'Callaghan R. and Wyckoff, A.W. (Eds), *Transforming Enterprise*, MIT Press, Cambridge, MA, pp. 375-397.

Dutton, W.H. and Piper, T. (2010), "The politics of privacy, confidentiality, and ethics", in Dutton, W.H. and Jeffreys, P.W. (Eds), *World Wide Research*, Oxford University Press, Oxford, pp. 223-240.

Dutton, W.H. and Blank, G. (2011), *Next Generation Users: The Oxford Internet Survey 2011*, Oxford Internet Institute, University of Oxford, Oxford.

Dutton, W.H. and Blank, G. (2013), *Cultures of the Internet: The Oxford Internet Survey 2013*, Oxford Internet Institute, University of Oxford, Oxford.

Dutton, W.H., Guerra, G.A., Zizzo, D.J. and Peltu, M. (2005), "The cybertrust tension in e-government: balancing identity, privacy, security", *Information Polity*, Vol. 10 Nos 1/2, pp. 13-23.

Guerra, G.A., Zizzo, D.J., Dutton, W.H. and Peltu, M. (2003), *Economics of Trust: Trust and the Information Economy*, DSTI/ICCP/REG/RD(2003)1, OECD, Paris.

Harter, A., Hopper, A., Steggles, P., Ward, A. and Webster, P. (2002), "The anatomy of a context-aware application", *Wireless Networks*, Vol. 8, pp. 187-197, available at: www.cl.cam.ac.uk/Research/DTG/publications/public/files/tr.2002.2.pdf (accessed 25 June 2013).

Head, S. (2014), *Mindless: Why Smarter Machines are Making Dumber Humans*, Basic Books, New York, NY.

Hook, L. (2013), "Weibo alters China's environmental debate", *Financial Times*, 4 March, available at www.ft.com/cms/s/0/a924440e-7fef-11e2-af49-00144feabdc0.html#slide0 (accessed 20 June 2013).

IoT (Internet of Things Special Interest Group) (2013), *A Roadmap for Interdisciplinary Research on the Internet of Things*, Special Interest Group on the Internet of Things, Technology Strategy Board, London.

ITU (International Telecommunication Union) (2005), *ITU Internet Reports 2005: The Internet of Things*, ITU, Geneva.

Kay, J. (2010), "Data sharing in geonomics–is it lawful?", in Dutton, W.H. and Jeffreys, P.W. (Eds), *World Wide Research*, Oxford University Press, Oxford, pp. 245-246.

Kirk, J. (2012), "Pacemaker hack can deliver deadly 830-volt jolt", *Computerworld*, 17 October, available at: www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt (accessed 20 June 2013).

Kling, R. (1978), "Value conflicts and social choice in electronic funds transfer systems developments", Working Paper of the Public Policy Research Organization, University of California Irvine, Irvine, CA.

Kortuem, G. (2013), "The internet of things in the context of sustainable cities: issues and challenges", abstracted in BCS, pp. 8-9.

Lewis, M. (2000), *The New Thing*, W. W. Norton & Company, New York, NY.

Löffler, M. and Tschiesner, A. (2013), "The internet of things and the future of manufacturing", Interview with McKinsey and Company, available at: www.mckinsey.com/insights/business_technology/the_internet_of_things_and_the_future_of_manufacturing (accessed 28 June 2013).

OECD (2012), "Machine-to-machine communications: connecting billions of devices", *OECD Digital Economy Papers*, No. 192, OECD Publishing, available at http://dx.doi.org/10.1787/5k9gsh2gp043-en (accessed 25 June 2013).

O'Hara, K. and Hall, W. (2013), "Web science", in Dutton, W.H. (Ed), *The Oxford Handbook of Internet Studies*, Oxford University Press, Oxford, pp. 48-68.

Rice, R.E., Shepherd, A., Dutton, W.H. and Katz, J.E. (2007), "Social interaction and the internet: a comparative analysis of surveys in the US and Britain", in Joinson, A.N., McKenna, K.Y.A., Postmes, T.

and Reips, U.-D. (Eds), *Oxford Handbook of Internet Psychology*, Oxford University Press, Oxford, pp. 7-30.

Rochlin, G.I. (1997), *Trapped in the Net: The Unanticipated Consequences of Computerization*, Princeton University Press, Princeton.

Spiekermann, S. (2013), "The self-regulation approach chosen for the development of the PIA framework for RFID", presentation at the BCS/OII Seminar on 'The Societal Impact of the Internet of Things', British Computer Society, 14 February.

Taylor, P. (2012), "Emerging tech: What is hot in IT", *Financial Times*, 29 August, available at: www.ft.com/cms/s/0/2dec25b6-f202-11e1-bba3-00144feabdc0.html#axzz2Ld4aXrL4 (accessed 20 February 2013).

Valéry, N. (2012), "Welcome to the thingternet: things, rather than people, are about to become the biggest users of the internet", *The Economist*, 21 November.

Weber, R.H. (2010), "Internet of things – new security and privacy challenges", *Computer Law and Security Review*, Vol. 26 No. 1, pp. 23-30.

Wilks, Y. (2007), "Is there progress on talking sensibly to machines?", *Science Magazine*, Vol. 318 No. 5852, pp. 927-928.

Wilks, Y. (Ed) (2010), *Close Engagements with Artificial Companions: Key Social, Psychological, Ethical and Design Issues*, John Benjamins Publishing Company, Amsterdam.

Ziegler, S., Crettaz, C., Ladid, L., Krco, S., Pokric, B., Skarmeta, A., Jara, A. and Kastner, W. (2013), "IoT6 – Moving to an Ipv6-based future IoT", *Future Internet Assembly*, pp. 161-172.

Zittrain, J. (2013), "Will the web break?", *Philosophical Transactions of The Royal Society*, Vol. A371: article 20120386, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1995059

Zuboff, S. (1988), *In the Age of the Smart Machine: The Future of Work and Power*, Basic Books, New York, NY.

Further reading

Droege, P. (Ed.) (1997), *Intelligent Environments*, North-Holland, Amsterdam.

Flood, G. (2013) "London Aims to be World's 'Smartest' City", *Information Week*, 6 March, available at www.informationweek.co.uk/government/leadership/london-aims-to-be-worlds-smartest-city/240150158 (accessed 25 June 2013).

Uckelmann, D., Harrison, M. and Michahelles, F. (Eds) (2011), *Architecting the Internet of Things*, Springer, Berlin.

About the author

William H. Dutton is Professor of Internet Studies at the Oxford Internet Institute, University of Oxford, where he is a Fellow of Balliol College, and Emeritus Professor at the University of Southern California. William H. Dutton can be contacted at: william.dutton@oii.ox.ac.uk

---

To purchase reprints of this article please e-mail: reprints@emeraldinsight.com
Or visit our web site for further details: www.emeraldinsight.com/reprints